Versión en español

Ilustración radical

Un mundo de fuentes abiertas por A.E. Freier

Ilustración radical: un mundo de fuentes abiertas (Introducción)

Es el año 20XX. Las personas llevan en su cuerpo pequeños ordenadores de alto rendimiento, conectados directamente a sus órganos sensoriales y, por tanto, al cerebro con sensores, pantallas y efectos sonoros. Estas interfaces cerebrales están conectadas a una red operada, supervisada y manipulada por un conglomerado de enormes empresas tecnológicas. Junto con los militares, las fuerzas del orden y una élite gobernante corrupta de las distintas regiones, se registran todos los pensamientos, acontecimientos, conversaciones y movimientos de la gente, se analizan, se manipulan y se vuelven a utilizar en su contra.

Potentes redes neuronales crean perfiles precisos de cada individuo, que luego se entregan a algoritmos igualmente potentes y guían a las personas hacia donde deben ir. La guerra, la pobreza, las epidemias aparecen para los individuos como su propia elección o, al menos, como un destino inevitable, impuesto sin piedad por una cosa grande, oscura y desconocida. Una gran parte de la población se ha rendido completamente al algoritmo y a sus amos, defiende su poder, habla su idioma y saluda cada 40 segundos aproximadamente conectando la interfaz a su cabeza.

La sociedad civil, tan poderosa en el siglo pasado, prácticamente se ha desintegrado. La prensa, los periodistas y los intelectuales (también importantes pilares de una sociedad libre no hace mucho tiempo) se someten abiertamente a las campañas. La búsqueda de la verdad se considera falsa y destructiva. La búsqueda de la verdad debe detenerse. De vez en cuando había individuos que exponían la nueva lógica y mostraban que, al fin y al cabo, sólo es obra del hombre y que se puede cambiar. Todos estos individuos están ahora en la cárcel huyendo o en la locura. Todos estos individuos fueron virtualmente ejecutados frente al público.

Los centros de poder son cada vez más pequeños, pero más poderosos. El 1% de la población mundial es dueña de todo. El resto recibe limosnas. Pero en la mayoría de los casos ni siquiera eso. 9 millones de personas mueren de hambre cada año, mientras que otras disponen de millones de veces el salario medio de un trabajador cada día. Entre el 99% de los desposeídos se libra una despiadada lucha por la supervivencia, caracterizada principalmente por el odio y el desprecio. El pensamiento y la acción política han dado paso a una lucha inútil por trivialidades inocuas para los

gobernantes. Las preferencias en el consumo o las argucias en el lenguaje cotidiano crean bandos irreconciliables que nunca dejarán de luchar entre sí. Y se pelean por NADA, por nada en absoluto.

Una terrible distopía, ¿no? ¿Cómo se ha podido llegar a esto? ¿Cómo hemos podido alejarnos tanto de los ideales de la Ilustración? ¿Y podemos hacer algo al respecto?

Sí se puede

Ilustración radical: un mundo de fuentes abiertas

¿El fin de la Ilustración?

En los siglos XIX y XX, se creía generalmente que el curso del mundo y la fortuna de las sociedades humanas evolucionan históricamente. Es decir, se asumía que siempre había una progresión y que todo se desarrollaba constantemente para mejor. Incluso en los estados tardoburgueses posteriores a la Segunda Guerra Mundial, se asumía que la siguiente generación lo tendría más fácil algún día. Se supone que los niños lo tienen mejor.

Por un lado, esta idea fue desencadenada por la enorme ganancia de conocimiento a través de las ciencias cada vez más sofisticadas. (Charles Darwin y su descubrimiento del origen de las especies deben ser mencionados en este contexto). Así como la popularización de la observación histórica en las humanidades a través de Hegel y posteriormente de Marx.

Por lo tanto, el conocimiento, la ética y la política no se desarrollaron a través de la providencia divina o de los destellos iluminados de unos pocos elegidos dotados, sino a través de un logro conjunto de la humanidad. El conocimiento y la experiencia se transmiten a través de generaciones y generaciones, se cuestionan, se desvían y se liberan de las aberraciones. La idea era positiva. Aunque este desarrollo no era en absoluto lineal, parecía ser la ley y cabía esperar un perfeccionamiento constante de las personas y las sociedades humanas.

El aumento cada vez más rápido de la industrialización, y la consiguiente aceleración del conocimiento de la física, podría obviamente hacer maravillas. Cada vez más trabajos pesados y desagradables son realizados por máquinas, la corriente eléctrica, los vehículos autopropulsados, la transmisión de información, imagen y sonido a miles de kilómetros anuncian un futuro glorioso.

Pero todo esto no quedó sin respuesta. Si todo se presenta de forma determinista, empírica y predecible, entonces no existe Dios. Las religiones rechazan naturalmente una visión histórica del mundo, ya que suelen suponer que hay un primer motor, un creador del mundo, o al menos que todo sucede en un ciclo, un ciclo. Desde este punto de vista, los cambios sólo pueden ser superficialidades y trivialidades, ya que al final todo se funde de nuevo en el Uno, en el origen.

También hubo (y hay) fuerzas reaccionarias. Estos rechazan la progresión, principalmente por razones personales, ya que supone la pérdida de poder, de propiedades, de derechos nobiliarios hereditarios o similares. O quieren creer que ciertos grupos (los suyos) tienen derechos ancestrales sobre ciertas tierras o derecho a la existencia en general.

La Ilustración, fundamento de toda sociedad burguesa (y en la que también tienen su base otros modelos de sociedad como el comunismo), es en el fondo un acontecimiento profundamente histórico y materialista. En los siglos XIX y XX, la Ilustración y la Revolución Francesa parecían acontecimientos irreversibles. Pero en el siglo XXI, las certezas se desmoronan.

La progresión ya no parece ser una promesa de salvación. La destrucción del medio ambiente y el rápido aumento de la desigualdad, la pobreza mortal, el hambre y la migración son constantes inalterables de la actual comunidad mundial. La advertencia de Günther Anders(1) de que la humanidad está siendo superada por su propia revolución tecnológica hace tiempo que dejó de ser un extraño argumento para novelas de ciencia ficción baratas.

A través de la especialización y la pericia, la digitalización, que ha cambiado la vida de todos en muy poco tiempo (no creo que uno se equivoque si sitúa el inicio de la digitalización en el año 2000 con la fundación de Google), se ha convertido en un monstruo mítico e inescrutable para el individuo.

La digitalización, que consiste al 100% en cálculos matemáticos empíricos y racionales, parece haberse convertido en un ídolo de los dioses. Arbitraria, imprevisible y cruel. Pero si sólo es obra del hombre, si sólo es calculable, entonces no puede ser la salvación de los grandes pensamientos de la Ilustración. ¿Quizás haya "libertad, igualdad y fraternidad" después de todo? ¿Quizás todo salga bien después de todo?

> (1) Günther Anders La antigüedad del hombre. Volumen I: Sobre el alma en la era de la segunda revolución industrial. C. H. Beck, Múnich 1956

Bienes comunes y capital

Una de las principales diferencias entre la época burguesa y todas las anteriores es el capital. Esto significa la propiedad privada de los bienes e ideas comunes. Los medios de producción, la tierra, las patentes y posiblemente también el trabajo humano pertenecen a personas privadas individuales que persiguen con ellos sus propios intereses privados. Esto crea una clase de capitalistas, por lo que esta forma de sociedad también se llama capitalismo. La idea liberal que subyace es que conduce a una competencia permanente de intereses y egoísmos individuales, que al final crea algo bueno y correcto para todos.

Si en un mundo idealizado y romántico de un Adam Smith, tal vez todavía sea posible pensar así, ya que allí todos tienen la misma posición de partida, en el mundo real se ve rápidamente que la acumulación de capital se produce. Las condiciones no son en absoluto las mismas. Donde se encuentre el capital, se acumulará más capital. Surgen estructuras centralizadas, monopolios, imperios, élites. El capitalismo se convierte en imperialismo. La violencia social se privatiza y los otros objetivos de la revolución burguesa, como la igualdad o la democracia, no pueden surgir o existir y se vuelven imposibles. La sociedad burguesa se suprime a sí misma.

Esto, como sabemos al menos desde Rosa Luxemburgo (2), no es una triste perversión contra la que se pueda luchar, sino que la acumulación de capital y la centralización del poder es inmanente a las sociedades basadas en la propiedad privada y sucede inevitablemente.

Se observan excesos extremos en las sociedades tardoburguesas de las últimas décadas. Bajo el concepto de neoliberalismo, desarrollado en los años 40, todo se privatiza, por así decirlo. Los pensamientos, los sentimientos, la infraestructura comunitaria, la política y los políticos, la guerra y la paz. Con la llegada de la digitalización y su completa privatización, hoy no hay lugar que no pertenezca a otros, que no esté completamente alejado de nosotros.

Por otro lado, están los denominados bienes comunes, un término un tanto vago (que por desgracia también es difícil de traducir al alemán, ya que lo más que se cuestionaría sería "Allgemeingut", que, sin embargo, sólo se refiere a los bienes). El término común se refiere a "lo que es de todos". Un ejemplo clásico es el paisaje. El paisaje siempre es de todos, porque aunque la tierra sea de una persona determinada, el paisaje siempre es de quien lo mira.

En nuestro mundo neoliberal, todos los bienes comunes se están privatizando gradualmente y, por tanto, son robados por definición. Uno de los ejemplos extremos es el sistema operativo. El sistema operativo, es decir, el software que hace que un ordenador sea utilizable, es uno de los grandes logros de la humanidad; ninguna empresa, y desde luego ninguna persona, lo ha creado ni puede venderlo.

Sin embargo, como es bien sabido, esto se hace, al igual que muchos otros productos, pensamientos, conocimientos creados por la humanidad son vendidos descaradamente de nuevo al pueblo, aunque hace tiempo que le pertenecen.

Por muy triste que parezca la situación en este momento, también muestra abiertamente cómo podemos superarla. Tenemos que conseguir transferir el capital de nuevo, o en los bienes comunes por primera vez. Esta idea no es nueva: "Los medios de producción en manos de los trabajadores". "Las casas, son de quienes las habitan", etc. Sólo se puede hacer por la fuerza. Pero la digitalización nos abre una posibilidad completamente nueva. La digitalización nos abre una vía para volver a poner los valores de la sociedad y la participación en ella, o por primera vez, en manos de quienes son la sociedad: nosotros, los ciudadanos.

La idea de esto, y es simple y radical, viene del desarrollo de software. ¡Es la idea de las fuentes abiertas!

> (2) Rosa Luxemburg - La acumulación de capital. Una contribución a la explicación económica del imperialismo. Buchhandlung Vorwärts Paul Singer, Berlín 1913

La inteligencia de las masas

En el curso del rápido progreso de la industrialización en el siglo XIX, surgió un nuevo fenómeno. Un cambio sin precedentes en la historia de la humanidad, la aparición de las masas. El centro de la vida cultural y, sobre todo, económica se desplazó del campo a la ciudad. Desde una comunidad social conformada durante siglos en el pueblo o la pequeña ciudad hasta los anónimos barrios obreros de masas en las cada vez más enormes y dominantes ciudades industriales y grandes.

Esto cambió fundamentalmente la sociedad. Las relaciones de clase pasaron de los campesinos y los señores al ejército de trabajadores, los proletarios, y a los que hacen trabajar a los trabajadores para ellos, los dueños de las fábricas y los capitalistas. Las masas son, pues, actores políticos. El siglo XX ha demostrado que las masas pueden desempeñar un papel muy ambivalente. Por un lado, se cometieron guerras totales y atrocidades increíbles en nombre del pueblo, de la comunidad o del propio grupo; por otro lado, se puso en marcha una tremenda democratización y destrucción de las estructuras de gobierno.

Hoy en día vivimos en una sociedad de masas, con todas las ventajas e inconvenientes y nos guste o no. Toda estructura gobernante, si quiere mantener a los gobernantes en el poder, debe controlar a las masas. Aparte de la violencia directa o la dependencia material, esto ocurre principalmente a través de los medios de comunicación. Si la radio ya desempeñó un papel nada desdeñable en la movilización de la población durante la Segunda Guerra Mundial, hoy en día la televisión y, en una medida decisiva, Internet también desempeñan un papel.

Internet (en el sentido más amplio) es ahora el actor más importante a la hora de tomar una decisión o ser llevado a tomarla. Puede hacer que a la gente le gusten ciertos productos y marcas o que odie a ciertos grupos, decide la guerra y la paz. Lo que ahora llamamos Internet está dominado por un puñado de gigantescas corporaciones tecnológicas que sólo se molestan en ocultar su conexión con el ejército y el poder, si es que lo hacen.

A primera vista, parece que hoy en día dirigir a las personas y manipularlas no supone ningún esfuerzo. Las masas parecen estúpidas y apáticas, en el mejor de los casos capaces de unirse en una turba. Pero si se mira más de cerca, se observa un fenómeno que casi siempre ocurre cuando las personas y las culturas están conectadas en red, el intercambio de conocimientos, la multiplicación de los mismos, la inteligencia de las masas.

¿Cuántas baldosas se colocaron y cuántos calcetines se tejieron con los vídeos de instrucciones de la WWW? ¿Cuántas preguntas contestadas y proyectos organizados? El conocimiento de los individuos es casi infinito en combinación, al menos en lo que respecta a nuestro pequeño mundo en nuestra pequeña tierra redonda. Esta combinación de conocimientos de la humanidad es increíblemente poderosa y, además de colocar las baldosas correctamente, una posibilidad de emancipación real y de auto-empoderamiento.

Esto no puede tener éxito si este conocimiento está en manos de unas pocas corporaciones, antes mencionadas, y pueden negar, impedir o manipular el acceso a voluntad. Este conocimiento despliega su poder a través del acceso libre y sin restricciones para todas las personas y a través de la dinámica que surge del hecho de que este conocimiento puede ser cambiado, combinado y renegociado a voluntad.

Para garantizarlo, se necesitan fuentes abiertas. Éstas garantizan la disponibilidad permanente y la transparencia permanente en cuanto a cómo ha cambiado la fuente y cuál es su origen. Las fuentes abiertas son una idea radical.

La libertad, ¿nuestro bien supremo?

Descartes, Spinoza, Rousseau y Kant y todos los demás grandes pensadores y filósofos de la Ilustración europea tienen un principio en común (y por tanto central en el pensamiento de la Ilustración): la autodeterminación del hombre. El hombre tiene un "derecho natural", un derecho humano, que se le ha dado en la cuna, por así decirlo. El hombre nace con libre albedrío y, por tanto, tiene el derecho natural de tomar sus propias decisiones y decidir sobre sí mismo.

Kant, en su ensayo "Respuesta a la pregunta: ¿Qué es la Ilustración?"(3), resumió la idea de la Ilustración con "Ten el valor de usar tu propia mente". juntos. La idea de independencia de la iglesia, las autoridades y los monarcas ha sido un componente central de toda sociedad moderna y burguesa desde entonces.

A diferencia de la modernidad, que es un producto puramente social y europeo, la Ilustración parece ser un proceso de emancipación universal inherente a toda la humanidad. La libertad no es negociable. La libertad es un derecho humano.

A diferencia de la libertad, la inmadurez no es una ley de la naturaleza; la inmadurez debe adquirirse. Desde la antigüedad, las personas pensantes se han preguntado por qué es posible que unos pocos puedan alzarse siempre por encima de la mayoría e imponerles su voluntad. Sería fácil para los muchos mandar a paseo al monarca o al señor.

Además de la apatía, siempre es el miedo el que mantiene a la gente en la esclavitud. Miedo a lo desconocido, miedo al enemigo, a las enfermedades, a las plagas, a Dios o a los demonios. Todos estos miedos son antiilustrados porque siempre apuntan a un núcleo irracional. La Ilustración europea contrarrestó el irracionalismo con el pensamiento empírico y racional, que puede describir todos los fenómenos reconocibles de la Tierra como una secuencia de causas y efectos. Esto significa que, al final, todo se vuelve investigable, categorizable y, por tanto, explicable. El miedo no tiene cabida allí y sólo puede formar parte de la experiencia individual, pero no tiene un estatus universalmente válido.

El racionalismo, como se ha mostrado anteriormente, no es en absoluto indiscutible. Pero todas nuestras sociedades industriales modernas de alta tecnología se basan en el conocimiento de que todo efecto tiene también una causa.

Pero, ¿sigue siendo eso cierto en nuestra época? ¿Es deseable que el individuo decida libremente? Ante las amenazas de la era que se avecina? Frente al calentamiento global, las epidemias y los conflictos inmanejables? ¿No es un dualismo anterior a la Ilustración, una clara división entre el bien y el mal mucho más adecuada para el reto del futuro que un libre albedrío que acabará por empujarnos a la ruina?

Esta visión del mundo es muy frecuente a principios del siglo XXI. Nietzsche la llama, no sin razón, moral de esclavos. Un simple determinismo moral que pueda explicar el mundo con un simple concepto de bien/mal es reaccionario en cualquier caso. Muchos de los defensores contemporáneos de este dualismo ideológico no se consideran en absoluto parte de la reacción, sino pioneros de un futuro desconocido. Es significativo que esta ideología incluya un mito de nuevos comienzos y el fin de la historia. De forma sistemáticamente dualista, el conocimiento de la humanidad se clasifica como "conocimiento tradicional" y se presenta como anticuado e incapaz de afrontar el futuro. Ya se ha planteado la cuestión de si los niños de Alemania deben seguir leyendo el Fausto de Goethe en la escuela.

Si uno piensa por un momento, sería fácil darse cuenta de que este pensamiento exige el fin de la razón y haría sonrojar incluso a cualquier idealista irracional y religioso.

¿Por qué la historia no debería seguir aplicándose, especialmente ahora, cuando el mundo se enfrenta a enormes desafíos? ¿Volvió Jesús? ¿Se ha cumplido una profecía maya? ¿Por qué la inmadurez y el conformismo han de ser garantes de la resolución de los cambios sociales sin precedentes que acaban de producirse? ¿O acaso no es más importante hoy en día cuestionar las cosas y llegar a un juicio autodeterminado?

Gracias a Hegel, se nos ha dado una herramienta excelente (aunque ciertamente difícil de usar) para describir el mundo en su totalidad contradictoria y confusa. La dialéctica. Este es nuestro tesoro, nuestra gran ventaja. Nunca debemos renunciar a ella. Sobre todo, no para un dualismo tecno-gnóstico de la Edad de Piedra, a la manera de Silicon Valley, que nos dice antes de tiempo, a través del smartphone, lo que es bueno o malo en la actualidad. ¡Abajo la inmadurez, arriba la libertad!

"Tengan valor para usar su propia mente".

> (3) Immanuel Kant: Respondiendo a la pregunta: ¿Qué es la Ilustración? En: Berlinische Monatsschrift, 1784

La dialéctica de la libertad

Entonces, si la libertad es nuestro bien supremo y no podemos prescindir de ella sin renunciar a nuestra existencia como seres humanos, ¿cómo la afrontamos? La libertad también significa peligro.

Esta es la confusa ambivalencia inherente a la libertad. Si no podemos recortar la libertad sin perderla, pero como seres humanos no podemos vivir sin un contrato que ponga la ley del más fuerte en su sitio y evite la arbitrariedad y la justicia por mano propia, ¿qué podemos hacer para resolver esta paradoja de la libertad?

Desde Aristóteles, existe un método racional y científico para que la humanidad no viva en la inmadurez ni en la arbitrariedad. La ética. A diferencia de la moral, que es su propia negación y

describe el estado del otro, el despreciable, como inmoralidad, la ética es el estudio científico de los hábitos, las costumbres y las prácticas.

Incluso los sofistas presocráticos consideraban intolerable que los seres humanos, como seres racionales dotados de libre albedrío, se guiaran únicamente por tradiciones, convenciones y conjuntos de reglas.

Aristóteles lo eleva a la categoría de ciencia que nos permite desarrollar racional y empíricamente y negociar repetidamente un contrato social. La ética presupone que el hombre es fundamentalmente racional y capaz de reflexionar. Si no fuera así, nunca habría podido salir del reino de la sensualidad y el misticismo ingenuos y, como un animal, sólo estaría a merced de sus impulsos e instintos.

La base de la ética es la virtud. Contrariamente a lo que se afirma en las revelaciones y en los despotismos, no hay reglas trascendentes establecidas ante la razón humana. Los 10 mandamientos de Moisés contradicen toda la ciencia y no son éticos. No en su contenido, ya que eso debe ser negociado, sino en su inmutabilidad dada por Dios.

Las constituciones que hoy esperamos como base de una sociedad moderna e ilustrada no surgieron por la gracia de Dios ni por la ocurrencia de una sola persona. Se luchó por ellas y se negociaron en un proceso histórico. Nuestra convivencia es el resultado de este proceso ético.

Pero, ¿qué significa esto para un mundo globalizado y digitalizado en transición? ¿Un mundo en el que los Estados nación ya no desempeñan ningún papel (aunque todo el mundo se aferre a ellos con pánico), en el que desaparecen las barreras lingüísticas y se produce una comunicación permanente en tiempo real?

Lo que sí se puede decir claramente es que se está produciendo un cambio radical. Que las antiguas normas, leyes y constituciones, que el antiguo contrato social tiene que ser renegociado. La ética es, pues, la ciencia del momento.

Los marxistas del siglo XIX ya intentaron crear una ética mundial. Lo llamaron internacionalismo, una palabra que ya lleva el nombre de nacionalismo. La situación en el siglo XXI es diferente, las fronteras arbitrarias se están disolviendo, está surgiendo una verdadera comunidad mundial.

Y para dominar esto, para desarrollar una ética mundial, necesitamos herramientas que nos permitan hacerlo. Deben ser, en el sentido marxiano, herramientas de auto-empoderamiento. Las estructuras digitales no deben estar en manos de individuos, empresas o naciones. La estructura debe ser libre.

Que hay que crear una base ética para la digitalización estaba claro para las personas inteligentes y racionales desde el principio. La base de la era de la información y la transformación digital se basa en el software. Además de los sistemas y programas patentados que aún hoy dominan, el software de código abierto surgió muy pronto. Un software que no pertenece a nadie, que puede ser desarrollado por todos y que garantiza la plena libertad y es perfectamente adecuado como herramienta ética de una nueva sociedad.

Por tanto, el software de código abierto no es un fenómeno técnico, sino ético y político. Una estructura para nuestro futuro.

La estructura del poder

¿Qué es lo que impide establecer una ética global? ¿Por qué la humanidad no se propone luchar por un estado en el que todas las personas puedan vivir con seguridad, libertad y autodeterminación?

Aparte de la conciencia de que tal estado es difícil o incluso imposible de alcanzar y la consiguiente falta de valor para atreverse a dar este paso hacia lo desconocido, son fundamentalmente las estructuras de propiedad y, por tanto, las estructuras de poder las que se interponen en el camino de tal paso.

A principios del siglo XXI, vivimos en una sociedad capitalista tardía. Como en todas las sociedades capitalistas, existe una clara división de las relaciones de poder. Hay una clase propietaria, que posee los medios de producción y, por tanto, tiene el control de todas las estructuras sociales, como el Estado, el ejército, la policía, los medios de comunicación, las infraestructuras, etc. Por otro lado, existe una clase sin propiedad en el sentido de que no es dueña de los medios de producción, que sólo puede "trabajar" para el beneficio de la plusvalía de otro y que, por lo tanto, está excluida de la ganancia, el significado y el éxito de su propio proceso de trabajo.

Por lo tanto, sigue existiendo una sociedad de clases. Si se observan las condiciones globales, no se puede pasar por alto el ejército de esclavos y proletarios (es decir, personas que no tienen más que reproducirse). Pero incluso en las sociedades industriales prósperas, la división entre los que tienen y los que no tienen se mantiene claramente, aunque a menudo esté oculta por la trivialidad y los privilegios.

Lo crucial, pues, es cambiar las relaciones de propiedad y liberar los medios de producción social de las manos de unos pocos. Los movimientos proletarios clásicos de los últimos 2 siglos, estaban convencidos de que había una especie de derecho histórico, que ese poder debía ponerse en manos de los trabajadores.

Pero ahora estamos en el umbral de una comunidad mundial completamente digitalizada. Pero esto también significa que los medios de producción, que hasta ahora han constituido la base de las estructuras de poder de esta sociedad, también se digitalizan. Las condiciones materiales previas de toda producción (herramientas, máquinas, fábricas) están ahora inextricablemente ligadas a un espacio virtual. Un espacio teóricamente infinitamente divisible e infinitamente reproducible que, aunque se basa en condiciones materiales previas, no es en sí mismo aprehensible como materia.

Una de las ideas básicas de una sociedad de código abierto es que el espacio virtual está tan estrechamente vinculado al mundo mecánico de la producción que, en cierto sentido, se crea una nueva herramienta. La parte virtual y digital de la herramienta domina la parte material. Si fuera posible situar las relaciones de poder en el espacio digital en contextos completamente nuevos,

esto también cambiaría las relaciones de poder materiales.

El factor decisivo aquí es que este poder no debe ponerse en nuevas manos, sino que debe ser utilizable, modificable y reutilizable como fuente abierta para todos.

En el caso de los programas informáticos, existe por tanto la siguiente definición de código abierto(4):

- El software (es decir, el código fuente) está disponible en una forma legible y comprensible para los humanos
- El software puede ser copiado, distribuido y utilizado como se desee
- El software puede ser modificado y transmitido en la forma modificada

Aplicado a nuestras relaciones reales de poder en un mundo digital, esto significa: las herramientas de poder, es decir, los medios de producción, pueden ser utilizados y cambiados por cualquiera, con cualquier propósito. La única condición es que las herramientas cambiadas puedan a su vez ser utilizadas y cambiadas libremente. Rápidamente se hace evidente que esta definición no tiene sentido en un mundo clásico y material. La situación es diferente si se asume que la materia y el espacio virtual se fusionan de forma inseparable. Entonces estas 3 demandas, en sí mismas poco espectaculares, son explosivos sociales.

Pensado hasta el final, este proceso promete tanto la libertad individual subjetiva como, debido a la retroalimentación permanente, la plena participación en el proceso social como tal.

> (4) Fuente -Wikipedia "Definition of the Open Source Initiative" - https://es.wikipedia.org/wiki/Open_Source

Tenedores de ética

¿Cómo podría concebirse una renegociación ética y, por tanto, científica de un contrato social (mundial) en un mundo digital de código abierto?

La dialéctica nos enseña que no hay una verdad trascendente a priori. Una civilización y los individuos están formados por ambivalencias y experiencias conflictivas, presupuestos y causalidades. Se caracterizan por ser verdades que se excluyen mutuamente. Para resolver esta paradoja, la humanidad en la antigüedad clásica, como se ha mostrado anteriormente, creó la ética como un instrumento racional para negociar estas contradicciones una y otra vez.

En el desarrollo de software de código abierto (y sólo allí) existe un proceso de bifurcación. Crear una bifurcación significa hacer una bifurcación de un programa. Se trata de un proceso sencillo y aburrido en el control de versiones, que debería garantizar que un programa básico idéntico pueda ser trabajado en direcciones diferentes e independientes.

Esto significa que cualquiera es completamente libre de copiar cualquier programa de código abierto y desarrollarlo según sus propias capacidades e intereses. A través del llamado fork, uno no sólo puede utilizar los conocimientos que han fluido en el programa original hasta ese momento, sino también adoptar futuros cambios y mejoras del programa original en su propio proyecto. También se crea un proceso de retroalimentación, que a su vez puede integrar las innovaciones de las empresas derivadas en el programa original.

Es concebible, por ejemplo, que un programa de control de bombillas pueda utilizarse en una horquilla para controlar motores eléctricos, y que las horquillas de este programa se utilicen a su vez en robótica o en el funcionamiento de presas, etc.

Este proceso, que a primera vista parece técnico, es una forma de comunicación extremadamente compleja y, como proceso, muy eficaz. Un tipo de comunicación que desempeña un inmenso papel en el curso histórico de la humanidad y que tiene un enorme poder gracias a la digitalización y a los conocimientos adquiridos al tratar con fuentes abiertas.

Así, el principio de bifurcación del desarrollo de software de código abierto es un instrumento eficaz, documentado y científico para trazar este proceso de comunicación. Combinada con la digitalización, esta comunicación se produce en tiempo real y permite así una renegociación, modificación y reajuste permanentes sin renunciar a las características establecidas y ya negociadas.

Para establecer este poderoso instrumento de negociación de una ética futura, se necesita una estructura completamente libre. Si se toma en serio la dialéctica, es imposible llevar a cabo un proceso de este tipo sin contradicciones y conflictos. Los juicios erróneos y las aberraciones también forman parte de la naturaleza humana. Por lo tanto, los errores y conflictos deben ser posibles y aceptados sin poner en peligro el proceso real.

Con los principios mencionados del movimiento de código abierto y el instrumento de las bifurcaciones y los forks en el espacio digital, ya disponemos de poderosas herramientas para dominar esta negociación de la ética.

La reconquista de la privacidad

En su contrato social, Kant ve la razón dividida en una razón privada y otra pública. La razón privada es el tipo de razón que podemos utilizar en la "oficina", es decir, una razón que está sujeta a fuertes restricciones y cuya observancia es necesaria para el buen éxito. La razón pública, por el contrario, es la del "erudito". Según Kant, éste debe ser libre y permitirse cuestionar y expresar todo.

Además de la razón en público, también existe el ámbito de la privacidad absoluta. Es decir, el ámbito de la familia, de los amigos o de uno mismo. En la antigüedad, esto se llamaba el oikos, el hogar. Mientras este ámbito no toque la esfera pública, por ejemplo, no infrinja ninguna ley de validez general, todo está permitido allí y se negocia en el propio oikos. No en vano la sexualidad y otras cosas que causarían una "molestia pública" se encuentran allí.

Pero, ¿qué ocurre en una sociedad digital en la que estos límites centenarios entre estas esferas se han disuelto prácticamente de la noche a la mañana? Esta disolución se produce, por un lado, a través de la autopublicación permanente en tiempo real en los llamados "medios sociales". Y en segundo lugar, y mucho más grave, mediante la vigilancia y el registro total, técnicamente factible y real, de todos los acontecimientos que tienen lugar en el espacio digital.

Dado que estamos en un mundo completamente digitalizado, todos los ámbitos de la vida también encuentran ahí una cartografía. No importa si se trata de la esfera privada del oikos o de la contemplación pública de un problema social. Por lo tanto, si todo se registra públicamente y, como todo el mundo sabe hoy(5), de forma permanente, esto significa la abolición completa de la privacidad, de la esfera privada, del oikos.

Esto es fatal. Si bien la razón pública y privada, simplemente y como en todos los tiempos, debe ser renegociada, la eliminación de la privacidad es una cesura en la historia de la humanidad y hasta entonces se consideraba un instrumento de tortura del panóptico en las instituciones penales y las cárceles.

Sin embargo, la privacidad y la esfera privada están inextricablemente ligadas a la libertad social e individual, así como a una vida digna en general. La reconquista de la intimidad es, pues, la lucha decisiva en el inicio de una digitalización total que ya no deja ningún espacio analógico.

Pero, ¿cómo se puede hacer esto? En el ámbito de la seguridad del software, existe el concepto de dominio militarizado y desmilitarizado. Se supone que cada dispositivo y cada programa que está conectado a la red mundial es (o puede ser) siempre atacado, leído, comprometido y manipulado. Todo lo que ocurre en Internet, en el espacio digital, tiene lugar, por tanto, en la zona militarizada y es, por definición, objeto de ataque permanente.

La respuesta a la pregunta de cómo establecer la privacidad en el espacio digital proviene lógicamente de la tradición militar. Es la criptografía. Desde el comienzo de los conflictos militares, la humanidad ha intentado alterar los mensajes importantes para que el enemigo no pueda evaluarlos.

Dado que todo lo que está en Internet puede ser potencialmente controlado por el "enemigo" (en este caso, el enemigo de la privacidad), es urgente que todo lo que sea privado, por muy poco interesante y trivial que sea, debe estar cifrado y criptografiado. La producción de una criptografía completa de la esfera privada es, pues, una de las tareas más importantes de la humanidad en la nueva época.

Además del reto de concienciar a la gente y ponerlo en práctica, una de las mayores dificultades es que se necesitan herramientas criptográficas para el cifrado y el descifrado. Estos no pueden estar en manos de individuos o grupos, sino que deben ser gratuitos y estar disponibles como fuente abierta. La propia herramienta criptográfica no debe contener ningún secreto. El secreto de la encriptación, la llave, debe estar en manos del individuo, igual que la llave con la que uno cierra la puerta de su piso antes de seguir sus preferencias privadas.

(5) Permanent Record (2019) Edward Snowden ISBN 9781529035650.

La democracia, ¿el mejor de los sistemas?

La digitalización es un fenómeno global, por lo que tiene el potencial de establecer una verdadera comunidad mundial igualitaria. Hoy en día, es fácil comunicarse en tiempo real con casi cualquier persona en cualquier parte del mundo. Las barreras lingüísticas se salvan sin esfuerzo gracias a los programas informáticos, puede surgir una lengua mundial formada por todas las lenguas conocidas, que podría ser completamente libre e independiente y, sin embargo, cada ser humano sería capaz de entender sin esfuerzo la lengua de cualquier otro ser humano. Este conjunto sería más que el internacionalismo de los comunistas, haría posible una comunidad mundial, una sociedad mundial.

Este fenómeno es ya omnipresente en la actualidad. Esto desencadena un contramovimiento igualmente extremo, una reacción. En todo el mundo se observa una recaída en el nacionalismo. El nacionalismo como ideología, y eso es lo que estamos tratando aquí, termina en la barbarie, como sabemos por la historia europea. Los detentores del poder reaccionan ante el flujo desenfrenado de información inherente a la digitalización con una impotente censura y manipulación de la información. (Y esto también se aplica a los Estados liberales, otrora burgueses, que hasta entonces al menos mantenían una apariencia de respeto a la libertad de expresión).

Por muy opresivos que sean el nacionalismo, la censura y la arbitrariedad, por muy fuerte que sea esta reacción, en un mundo completamente globalizado y digitalizado estos fenómenos no podrán desempeñar ningún papel a largo plazo. Incluso ahora, al comienzo de este nuevo desarrollo, parecen indefensos y patéticos, pero aún más peligrosos por ello.

Pero si es posible establecer una comunidad mundial, ¿cómo podría ser un sistema político que le haga justicia? En la política clásica (es decir, la ciencia de la convivencia) y en la filosofía política, se suele dividir entre un sistema ideal y otro que sería aplicable en condiciones reales.

En la antigüedad y hasta principios de la época moderna, las formas concebibles de la sociedad se conocen típicamente como un grupo de seis con tres formas buenas y tres malas. Las formas buenas son en su mayoría la monarquía, como el gobierno de uno pero bueno, la aristocracia como el gobierno de unos pocos pero capaces, la política como el gobierno de muchos pero dignos. Las formas malas son sobre todo la democracia como gobierno del pueblo y por tanto de los pobres, la oligarquía como gobierno de unos pocos ricos y la tiranía como gobierno de un déspota, un tirano.

En los tiempos modernos, la cortesía se transforma lentamente en el mucho más complejo liberalismo o democracia representativa, que equivale al gobierno del Estado. La democracia clásica se transforma en comunismo, la dictadura del proletariado. Desde la Ilustración y la aparición del individuo como actor político, surgió otra forma política concebible, el anarquismo. Mientras que en la antigüedad la anarquía era simplemente la ausencia del Estado, es decir, la inexistencia de la comunidad, con el advenimiento de los derechos humanos pasó a entenderse como la ley natural y el individuo soberano, como regla de ese mismo individuo, en beneficio de todos.

Cicerón ya reconocía que una regla pura de las 6 formas descritas nunca haría justicia a una sociedad compleja y que las formas individuales siempre se mueven, en una tendencia descendente, hacia lo peor y hacia la inestabilidad. Así, propuso una conexión de todas las formas, que podría interpretarse como una forma temprana del enfoque dialéctico.

Ahora bien, en política no existe un dualismo moral que permita distinguir fácilmente las formas buenas de las malas de la sociedad. En una sociedad moderna muy compleja, y más aún en una comunidad mundial, hay tantos intereses individuales legítimos y situaciones de partida fundamentalmente diferentes que resulta imposible establecer un sistema que pueda hacer justicia. La única posibilidad que existe es la aplicación coherente del enfoque dialéctico.

Como es imposible que las contradicciones se unifiquen, hay que aceptarlas como contradicciones. En la dialéctica, existe el triple paso de tesis, antítesis y síntesis. En este proceso, las partes contradictorias, tesis y antítesis, se disuelven en la síntesis. Cómo puede tener éxito esta síntesis en un mundo altamente complejo es un reto para la humanidad. También ahí, y sobre todo ahí, la digitalización de las fuentes abiertas puede beneficiarnos enormemente.

El software y las fuentes abiertas

Si asumimos, como hacemos aquí, que el mundo entero y todos los ámbitos de la sociedad están o estarán digitalizados, entonces se pone de manifiesto un logro cultural de la humanidad: el software. El software y los lenguajes de programación ya no son un simple subproducto de una nueva tecnología, sino que son la columna vertebral y la base de este nuevo mundo digitalizado.

Los lenguajes de programación son herramientas de información artísticas que no tienen nada que envidiar a los lenguajes clásicos de alto nivel en cuanto a complejidad y contenido. Todo lo que hoy llamamos digitalización o Internet se basa en el software. Cada aplicación, cada sitio web, cada control de una máquina, cada control de una central nuclear, simplemente todo lo que es digital de alguna manera (y en una sociedad digital eso es todo) se controla a través de un software, es decir, a través de un documento escrito creado por humanos. En cierto modo, es literatura en un sentido completamente nuevo.

Cuando te das cuenta de esto, queda claro que es un instrumento de poder, si no EL instrumento de poder de una nueva era. Los programas informáticos pueden cambiar, manipular, eliminar y crear la base de la sociedad de la información, es decir, la información, a voluntad. Por un lado, esta es su tarea, por otro lado, esto deja un enorme espacio para los abusos de todo tipo.

La pregunta es, por tanto, cómo se puede conseguir que las personas, a pesar de sus diferentes condiciones previas y capacidades, puedan convertirse en propietarios del software que utilizan y deben utilizar. La respuesta es que este software debe descentralizarse hasta tal punto que al final no pertenezca a nadie, o positivamente que sea de todos.

Este principio parece bastante abstracto e inaplicable. Pero hay una lógica sorprendentemente sencilla que puede hacer que funcione. Y eso es, como cabría esperar, software de código abierto. Por lo tanto, no todas las aplicaciones de código abierto son igualmente emancipadoras, pero la

estructura que hay detrás es poderosa y tiene la capacidad de lograr este objetivo.

A principios del siglo XXI, no se reconoce la relevancia de las estructuras de código abierto. El software libre se considera un producto de nicho, que es gratuito pero suele ser de baja calidad. La idea que la sustenta parece demasiado simple para tener valor social. Pero si se examina la definición con más detenimiento, muestra un enorme poder.

Como se ha mencionado anteriormente, hay tres definiciones básicas como requisitos previos.

En primer lugar, la accesibilidad es gratuita. La primera definición es: "El software está en una forma que puede ser leída y entendida por los humanos". Esto significa que cualquier persona que domine el lenguaje de programación correspondiente puede entender lo que está escrito y modificarlo de cualquier forma. Esto implica que es esencial para una educación general en un mundo digitalizado que se domine una de estas "nuevas" lenguas. Si esto fuera así, sería posible una completa transparencia de las estructuras definidas anteriormente como instrumentos de poder. Como no todo el mundo puede hacerlo igual de bien, en el caso de un código fuente completamente libre basta con que un número suficientemente grande de la zoon politikon, según sus capacidades individuales, se encargue de este examen de los instrumentos. Como el código fuente es abierto, puede tratarse de un grupo enormemente amplio de expertos que ni siquiera tienen que conocerse entre sí para realizar esta tarea.

La segunda definición es: "El software puede ser copiado, distribuido y utilizado como se desee. Por un lado, esto garantiza la disponibilidad permanente y, por otro, supone un alejamiento radical de la propiedad privada del software. El software moderno se entiende como un logro humano y, por tanto, no puede tener dueño. Si se combina con la primera definición, el potencial que hay detrás queda claro y se llega a la tercera definición: "El software puede ser modificado y transmitido en la forma modificada".

Si todo el mundo tiene acceso sin restricciones a cualquier programa informático y puede modificar estos textos de cualquier forma y, a su vez, ponerlos a disposición de todo el mundo sin restricciones, se crea una increíble combinación de conocimientos. También, de forma bastante dialéctica, se resuelven las contradicciones. Si las aplicaciones son inútiles y equivocadas para un grupo, entonces pueden hacer cambios en su beneficio sin condescender con el grupo que se lleva bien con la aplicación original.

Podría surgir una síntesis dialéctica, un auténtico pluralismo.

Federal, Descentralizado

George Orwell, uno de los pensadores más profundos e influyentes del siglo XX, describe en su emblemático libro "1984"(5) un mundo de totalitarismo centralista que impregna la totalidad de la vida individual y comunitaria. Aunque su libro es una novela, es un análisis perspicaz de las sociedades de masas de la modernidad tardía.

Que esto no es pura ficción y que afecta fatalmente a las personas dentro y fuera de las sociedades en cuestión ha sido demostrado por muchos ejemplos en la historia reciente, algunos de ellos los más crueles. La base de estos totalitarismos, tanto en la visión de Orwell como en las versiones históricas reales, es siempre un centralismo radical. Un centralismo que no deja espacio para la autorrealización individual o un modelo de sociedad pluralista que tenga en cuenta las contradicciones y peculiaridades de una sociedad de masas compleja y moderna.

Por lo tanto, se puede asumir que, como tendencia, todas las sociedades confusas y alienadas se mueven hacia el centralismo y el totalitarismo. Como se reconoció desde el principio, la mayoría de las primeras constituciones burguesas y liberales se basaban en una idea de federalismo, descentralismo e individualismo.

La sociedad digital emergente también tiene esta tendencia totalitaria. Hoy en día, unas pocas empresas tecnológicas unidas en forma de monopolio dominan gran parte de Internet en un sentido totalitario. No sólo todas las plataformas digitales y, por lo tanto, toda la comunicación e interacción social que tiene lugar en ellas están bajo el control de dicho monopolio, sino que además los dispositivos finales y la estructura técnica no están en gran medida en manos de quienes tienen que utilizarlos.

El hecho de que el control y la vigilancia exhaustivos en el sentido orwelliano se están llevando a cabo con él está ya bien probado y documentado y es conocido por una gran parte de la gente. Así, la sociedad digitalizada avanza hacia los mismos fatalismos que la sociedad tardoburguesa. Muy probablemente con las mismas crueles consecuencias. Así que tenemos que hacer algo.

También en este caso, las fuentes y el software abiertos nos proporcionan poderosas herramientas. Uno de los fundamentos más destacados de esta estructura es el descentralismo. Como se ha descrito anteriormente, las fuentes abiertas pueden ser manipuladas y modificadas a voluntad por cualquiera. Así, pueden adaptarse a las necesidades propias o a las de un grupo sin poner en peligro los intereses de otros grupos o individuos.

Esto resulta especialmente claro en la interacción social e interpersonal de los individuos. Hoy en día, esto se ha trasladado en gran medida al espacio digital. Este tipo de comunicación es especialmente sensible y digna de protección, ya que se refiere a la esfera privada de las personas, que por definición no está destinada al público. Es fácil ver que esta protección de la privacidad no es posible en un espacio digital totalitario y centralizado como el que encontramos hoy. En una totalidad, todo, incluso la comunicación más privada, es público per se.

El problema sólo puede resolverse descentralizando la estructura subyacente. Basado en el movimiento del código abierto, actualmente está surgiendo la llamada Internet federada (a menudo llamada Fediverse en el lenguaje cotidiano). En esta federación, se supone que la comunicación social en el espacio digital, por ejemplo, se limita a unos pocos procedimientos estándar. Se definen como estándares abiertos y son aceptados por todos los actores de la red federada. Esto conduce a un grado enormemente alto de libertad individual y privacidad consistente.

Veamos los llamados medios sociales como ejemplo. Las redes sociales son el lugar donde se produce una gran parte de la comunicación privada. Hoy, estos medios están en manos

monopólicas y totalitarias. Sin embargo, la estructura de esta comunicación se basa en unas pocas acciones estandarizadas. Así, hay que publicar o postear, comentar otras publicaciones, afirmar o gustar, republicar el contenido de otros, el llamado compartir o comunicación directa, chatear, etc.

Así, si estas acciones se basaran en normas abiertas comprensibles para cualquier actor, sería posible que cualquier entidad independiente que se adhiriera a estas normas abiertas se comunicara con cualquier otra entidad con las mismas normas de la manera indicada anteriormente.

En un caso extremo, sería concebible que cada individuo operara una instancia de este tipo en su propio hardware como una instancia privada y aún así pudiera comunicarse con las otras instancias. Dado que los requisitos para el funcionamiento de este tipo de estructuras no están al alcance de todo el mundo, los actores sociales como las asociaciones, los municipios, las universidades, los grupos individuales o los individuos podrían operar esta estructura abierta.

Como el software subyacente y las normas acordadas están disponibles como fuentes abiertas, también pueden ser utilizadas por todos. Federal, descentralizado.

> (5)Diecinueve ochenta y cuatro. Penguin, Londres, 2021, (edición original actual) ISBN 978-0-24-145351-3.

Criptografía individual

En la teoría clásica del contrato à la Rousseau o Hobbes, es decir, en el contractualismo, se supone que una sociedad se desarrolla a partir de un estado primordial. En este estado primordial, todavía no hay sociedad ni contrato; es un estado de racionalismo amoral en el que cada persona debe buscar su propio bienestar para sobrevivir. Es la constelación de "todos contra todos". Si la sociedad surge de un estado primordial, nos encontramos con un estado inicial justo, o más profanamente, en la duda, todos pueden matar a todos. La desigualdad sólo surge con la propiedad.

Según esta teoría, una sociedad está formada por un contrato, y este contrato surge de la necesidad. Ahora bien, no hay que compartir la teoría del contrato, pero muestra bien en qué condiciones surgen las (nuevas) sociedades.

También hoy nos enfrentamos a la renegociación de una sociedad. Sin embargo, no desde un estado primordial, sino como una transición de una sociedad burguesa a una sociedad digital. No se puede hablar de un estado inicial justo, ya que la sociedad en declive, tardomoderna y acumulada, se caracteriza por la desigualdad en grado extremo. Como ya se ha demostrado, esta desigualdad extrema ya se refleja en la nueva sociedad a través de la aparición de los monopolios digitales.

El estado de racionalismo amoral (Hobbes lo llama "homo homini lupus" - el hombre es, para el hombre, un lobo), por otra parte, es fácil de observar hoy en día. Todo el espacio digital es un área

"militarizada". En caso de duda, todo el mundo ataca a los demás; prácticamente no hay región en la que uno esté a salvo. En cuanto se conecta un dispositivo a Internet, es público y vulnerable. Todas las tardes acogedoras, con la tableta y la televisión inteligente en el sofá, en realidad tienen lugar con la cartera abierta y en ropa interior en el mercado.

Los anticuados monopolios de la sociedad capitalista no son sólo actores amorales (como todos los demás), sino que son lobos en vías de convertirse en el nuevo Leviatán(6). Lobos con enorme poder.

Para lograr una sociedad sin el estado de racionalismo amoral y desigualdad monopolizada, también necesitamos herramientas. Herramientas que no quieren acabar fundamentalmente con el estado de "todos contra todos", sino reconocerlo y hacerlo inofensivo en la estructura.

Esa herramienta es la criptografía. La criptografía existe desde que las personas se oponen como grupos conflictivos. Se han ganado bastantes guerras encriptando la información propia de forma que el enemigo no pudiera entenderla, o desencriptando la información del enemigo. Dado que nos encontramos en una zona "militarizada" en el espacio digital (y en la consiguiente sociedad de la información), la encriptación de la propia información privada es esencial para todo actor e indispensable para una vida digital libre y autodeterminada.

Esto significa que, por primera vez en la historia de la humanidad, hay que luchar por el derecho a la criptografía individual. Individual en este contexto significa que el cifrado y descifrado de la propia información sólo puede ser realizado por el propio individuo. Por lo tanto, no hay instancias intermedias. En lenguaje llano, la información sólo está disponible para los actores individuales a los que va dirigida. Esto se llama encriptación de extremo a extremo.

Mientras nos encontramos en la fase de transición de la sociedad burguesa a la digital, se libra una batalla por el derecho a la criptografía individual. Esta batalla se está librando de forma tan encarnizada y brutal que el término "criptoguerra", es decir, guerra criptográfica, se ha convertido en lenguaje común.

Los oponentes de la criptografía son, como era de esperar, el monopolio digital establecido y las estructuras anticuadas de las sociedades tardoburguesas, como el Estado y los ejecutivos que defienden las antiguas estructuras de poder. La justificación de esta reacción no suele ser la conservación del poder, sino la maldad de los seres humanos. Hay que vigilar a la humanidad porque, de lo contrario, se destruirá a sí misma. El mantra sagrado y la trinidad en este contexto suele ser "terroristas, nazis, pederastas" y la amenaza populista de que sin la protección patriarcal estaríamos indefensos ante estos fenómenos patológicos. Sin embargo, lo que se pretende es un prejuicio colectivo de todos, como instrumento de poder.

Como se ha mostrado anteriormente, la criptografía individual también supone actores amorales, pero muestra claramente que la protección contra el racionalismo amoral de otros sólo puede ser la protección de la propia información. Asimismo, es crucial para romper con las estructuras de poder anticuadas y capitalistas de la vieja época.

(6)Thomas Hobbes: Leviatán. Cambridge University Press, Cambridge 1996, ISBN 978-0-521-56797-8.

Criptografía práctica

La descentralización y la criptografía individual son requisitos esenciales para hacer posible una vida emancipadora y autodeterminada para todas las personas en el espacio digital. Mientras que la descentralización de la interacción digital es un procedimiento estructural y puede lograrse proporcionando procedimientos y normas estándar como fuentes abiertas independientes del individuo, la criptografía individual es también un problema individual.

La historia de la criptografía moderna (tal y como se utiliza hoy en día en el espacio digital) es relativamente antigua(7) y no tiene mucho que ver con la digitalización. La criptografía moderna es un campo especial muy complejo de las matemáticas superiores y requiere una enorme capacidad de abstracción y un profundo conocimiento de las secuencias numéricas, los cifrados y los procedimientos matemáticos.

Por tanto, su conocimiento está reservado a un grupo muy reducido de personas. Teniendo esto en cuenta, un criterio para un buen método de cifrado no es sólo la protección contra el descifrado por parte de terceros no autorizados, sino también la operatividad sensata y fácil y el manejo sin complicaciones del método por parte de usuarios sin los correspondientes conocimientos matemáticos.

Dado que la criptografía individual, el verdadero cifrado de extremo a extremo, debe ser siempre realizada por el individuo, ya que no puede haber instancias intermedias, esto supone un enorme reto para una sociedad digital emancipada.

Hasta el desarrollo de la criptografía moderna en el siglo XX, todos los métodos de cifrado se realizaban mediante el principio de "seguridad a través de la oscuridad". El método de encriptación en sí tenía que ser poco claro. Todos los participantes que quisieran tomar parte en la comunicación cifrada debían conocer el procedimiento de descifrado. Esto significaba además que cualquier tercero que conociera este modo de cifrado podía descifrar todo el contenido cifrado con este método. Así que este proceso es muy inseguro y fácil de comprometer. Y, por supuesto, el secretismo del proceso contradice por completo la idea de las fuentes abiertas. El proceso criptográfico debe ser urgentemente de código abierto y verificable.

Así, a mediados del siglo XX, surgió un método basado en el intercambio de claves. Por tanto, el secreto necesario para un cifrado ya no era el procedimiento en sí, sino que se basaba en una clave secreta que debía ser conocida por el emisor y el receptor. Por un lado, esto permitió revelar el procedimiento, permitiendo así un examen científico de este método, y por otro lado, el compromiso de una clave no puso en duda todo el procedimiento.

En este contexto, tanto en los cifrados matemáticos como en los digitales, la clave suele ser una cadena de caracteres larga y compleja que no se puede adivinar ni calcular con un esfuerzo

razonable. Así, en el espacio digital, suele ser simplemente un archivo el que sirve de secreto. (Por supuesto, la criptografía moderna es mucho más compleja de lo que sería posible presentar aquí).

La desventaja de este método, también llamado cifrado simétrico, es que la propia clave debe transmitirse al destinatario. Dado que el cifrado y el descifrado utilizan la misma clave, el emisor y el receptor también deben estar en posesión de esta clave. Si en el espacio analógico todavía es concebible que la clave correspondiente pueda ser intercambiada por un mensajero de confianza o un encuentro personal, esto es sencillamente imposible en el espacio digital con miles de millones de potenciales interlocutores de comunicación.

En 1976, Whitfield Diffie y Martin Hellman desarrollaron un método de cifrado asimétrico(8). Este método es excelente para proporcionar un cifrado de extremo a extremo sin concesiones en el espacio digital, incluso si los participantes en la comunicación no se conocen entre sí. Hoy en día, este principio es también el procedimiento estándar para toda comunicación individual y cifrada en Internet.

Este tipo de cifrado se basa en la idea de que cada participante tiene dos claves. Una clave privada que vale la pena proteger y una clave pública que es conocida por todos los demás. La clave pública, como su nombre indica, se pone a disposición del público y sólo puede cifrar. Por lo tanto, una clave pública no puede descifrar nada, ni siquiera los contenidos que fueron cifrados con la misma clave.

En cambio, la clave privada, que es digna de protección, sólo ofrece la posibilidad de descifrar. Por lo tanto, los contenidos cifrados con una clave pública sólo pueden descifrarse con la correspondiente clave privada. Por lo tanto, si se quiere hacer posible una auténtica criptografía individual, es necesario que cada participante individual en la comunicación digital posea al menos un par de claves de este tipo y lo gestione él mismo. Si la clave privada se pierde o terceros no autorizados acceden a ella, el contenido encriptado se pierde irremediablemente o queda comprometido.

Este es sin duda un problema al que se enfrenta una sociedad digitalizada. Si toda la estructura de una sociedad digital abierta existe como fuente abierta y, por lo tanto, está disponible en todo momento, está en la naturaleza de las cosas que un secreto, que es lo que es la clave privada, sólo sea conocido por el individuo al que se dirige el contenido privado.

En el espacio analógico, se da por supuesto que las zonas privadas, como el hogar, están protegidas por una llave y que hay que tener el cuidado correspondiente. Dado que un secreto como una llave no puede depositarse simplemente en una estructura abierta, esta conciencia también tendrá que prevalecer en una sociedad digital, para un área privada digital. Sobre todo porque allí no hay ni cerrajeros ni palancas.

(7) Claude Shannon: The Mathematical Communication Theory of Cipher Systems. En: On - Off: Selected Writings on Communication and Message Theory. 1ª edición. 1949 Brinkmann y Bose, Berlín 2000, ISBN 3-922660-68-1,

(8) W. Diffie, M. E. Hellman: New Directions in Cryptography. En: IEEE Transactions on Information Theory. Vol. 22, No. 6, 1976

Version #4
Erstellt: 10 November 2022 14:31:41 von reverend
Zuletzt aktualisiert: 20 November 2022 14:14:06 von reverend